

**COMMITTEE ON GOVERNMENT REFORM**  
**TOM DAVIS, CHAIRMAN**



**NEWS RELEASE**

**For Immediate Release**  
**September 22, 2006**

**Contact: David Marin**  
**(202) 225-5074**

**Davis Statement on Missing Commerce Computers**

**Washington, D.C.** – Government Reform Committee Chairman Tom Davis (R-VA) issued the following statement today in response to information he received yesterday from Commerce Secretary Carlos M. Gutierrez. The Department informed Davis that 1,137 laptops had been lost, misplaced, or stolen since 2001. It also is missing 46 “thumb drives” and 16 hand-held computers. 672 of the missing laptops were from the Census Bureau. Of those, 246 contained personally identifiable information.

The information was requested by Davis and Ranking Member Henry Waxman (D-CA) in a July 10 letter. Identical letters were sent to all Cabinet agencies, as well as the Social Security Administration and the Office of Personnel Management. The Committee continues to receive and review the responses from those agencies, and will issue its overall findings in the near future:

**“Perhaps the most shocking thing here is that the public might not have ever known of these breaches, and their scope, if we hadn’t specifically asked for the information,” Davis said. “Why aren’t these inventories taken automatically, instinctively?**

**“We don’t yet know exactly how many computers were lost, or whether personal information was compromised. The Secretary has assured me that getting that information is priority number one, and I’m confident he’ll get his arms around the problem.**

**“But the American people deserve better from their government. I plan to immediately pursue whatever legislative fixes are necessary to make these losses less prevalent, and make sure that when they do occur, the right people know and act immediately on that information, and share it with everyone potentially at risk.**

**“My Federal Information Security Management Act (FISMA) was aimed at protecting the government’s information, operations, and assets. It requires the**

head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level. FISMA requires agency program officials, Chief Information Officers, and Inspectors General to conduct annual reviews of the agency's information security program and report the results to OMB. And every year, the Government Reform Committee releases its FISMA scorecard, grading each agency, A through F. Commerce went from F in '04 to D+ in '05.

“One FISMA provision requires all agencies to report incidents to a Federal incident response center, known as US-CERT, located within the Department of Homeland Security.

“I'm interested in learning whether that happened in this case, and if so, what action was taken. We may need to update the law regarding notification of Congress, and the Government Reform Committee in particular. We would not have learned of this unless we asked, and I'm surprised agencies don't have this information at hand. That shows we still have a long way to go on agency data security.

“In addition, we need to strengthen the laws regarding notification of the public. That's why I previously introduced HR 5838, The Federal Agency Data Breach Notification Act. Congress has been working on *private* sector breach notification legislation. But federal agencies hold massive amounts of sensitive personal information on every person in the US, including health records, tax returns, and military records. There is no policy, procedure, or standard for notifying citizens when sensitive personal information held by a federal agency is compromised.

“In light of the VA breach and the subsequent delay in public notification, as well as a number of other incidents involving federal agencies, a strong government-wide policy is required. My bill would require OMB to establish policies, procedures, and standards for agencies to follow in the event of a data breach. Given these recent disclosures, I intend to revisit that bill and augment it as necessary. If we're going to ask and sometimes demand information from the public, we owe them a better way of knowing when that information goes missing.

“As we receive and review information on data breaches from all agencies, we must remember that we are striving for a 21<sup>st</sup> century government to meet 21<sup>st</sup> century challenges and fight 21<sup>st</sup> century enemies. And information is the oil of the 21<sup>st</sup> century.

“The reality is, we are incapable of storing, moving and accessing information. No government does these things well, especially big governments. We spend tens of billions of dollars a year on information technology. You'd think we could share information by now. But we are still an analog government in a digital economy and culture.”

###